Olha Zubenko
D.S. Tymofieiev, research supervisor
N.V. Poperechna, language adviser
National TU «Dnipro Polytechnic», Dnipro, Ukraine

Categories of Controlling Risk Management

Annually organizations all across the world lose billions of dollars because of the threat posed by authorized personnel. That includes sabotage, human error, negligence and exploitation by outsiders to consider. There are some approaches how to decline the risk of data leakage by controlling personnel. To protect data and system organizations should use the following clauses.

Classification and Analysis. First, you should classify information by availability, confidentiality, integrity using CIA rating and identify system boundaries.

Identification of Controls. After classifying valuable information establish control standards to impact categories: high, medium and low. Pay special attention to controlling the categories.

Human Resources. Lots of crimes committed by insiders were suspected by employees. Personnel should do background checks of employees, people in high positions, service staff. Take their signs in document about security policies.

Security Awareness Program. Personnel must be aware of security policies. Make the introductory briefing or informational program with tests for staff. Give personnel the chance to ask questions of advocating security initiatives.

Access Control. Control access of personnel. Make the structure of classes with different types of roles. Check the different access to avoid the mistakes. Create the application for remote access and for providing data confidentiality. To prevent unacceptable file downloads use terminal servers to provide remote access to data and systems.

Social Engineering. Provide the safety of information. Create certain processes for protection of information, ensure an escalation path and spread the information about techniques used by social engineers.

Implementation. Next step is to bind business risks of the organization and information security controls. The simple process of applying controls based on sensitivity of data and impact ratings will appeal most compliance problems. All possible changes should be agreed by information security managers.

Audit. To keep data and valuable assets safeguarded it is necessary to take a hard look at who has access to data and also monitor systems. Compare a list of the current personnel of the company with their active accounts.

In conclusion, it should be noted that there is a real threat from authorized personnel in organizations that can cause lots of damage. Although trust to employees is important, control is an integral part of information security.